

Tsvilii, Olena

## Article

# Cybersecurity regulation : cybersecurity certification of operational technologies

Technology audit and production reserves

## Provided in Cooperation with:

ZBW OAS

*Reference:* Tsvilii, Olena (2021). Cybersecurity regulation : cybersecurity certification of operational technologies. In: Technology audit and production reserves 1 (2/57), S. 54 - 60.  
<http://journals.urau.ua/tarp/article/download/225271/225603/514516>.  
doi:10.15587/2706-5448.2021.225271.

This Version is available at:

<http://hdl.handle.net/11159/6806>

## Kontakt/Contact

ZBW – Leibniz-Informationszentrum Wirtschaft/Leibniz Information Centre for Economics  
Düsternbrooker Weg 120  
24105 Kiel (Germany)  
E-Mail: [rights\[at\]zbw.eu](mailto:rights[at]zbw.eu)  
<https://www.zbw.eu/>

## Standard-Nutzungsbedingungen:

Dieses Dokument darf zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden. Sie dürfen dieses Dokument nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen. Sofern für das Dokument eine Open-Content-Lizenz verwendet wurde, so gelten abweichend von diesen Nutzungsbedingungen die in der Lizenz gewährten Nutzungsrechte. Alle auf diesem Vorblatt angegebenen Informationen einschließlich der Rechteinformationen (z.B. Nennung einer Creative Commons Lizenz) wurden automatisch generiert und müssen durch Nutzer:innen vor einer Nachnutzung sorgfältig überprüft werden. Die Lizenzangaben stammen aus Publikationsmetadaten und können Fehler oder Ungenauigkeiten enthalten.

## Terms of use:

*This document may be saved and copied for your personal and scholarly purposes. You are not to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public. If the document is made available under a Creative Commons Licence you may exercise further usage rights as specified in the licence. All information provided on this publication cover sheet, including copyright details (e.g. indication of a Creative Commons license), was automatically generated and must be carefully reviewed by users prior to reuse. The license information is derived from publication metadata and may contain errors or inaccuracies.*



<https://savearchive.zbw.eu/terms-of-use>

Olena Tsvilii

# CYBER SECURITY REGULATION: CYBER SECURITY CERTIFICATION OF OPERATIONAL TECHNOLOGIES

*The object of research is the system and schemes of conformity assessment (certification) of cybersecurity of operational technologies (OT), as a set of rules and procedures that describe the objects of certification, determine the specified requirements and provide a methodology for certification. The terminological base and conceptual apparatus of the study of cybersecurity certification of operational technologies are based on the international standard ISO 17000:2020 Conformity assessment – Vocabulary and general principles. Cybersecurity certification systems and schemes are based on assessment standards, the choice and application of which is not unambiguous and historically has many interpretations and application mechanisms. These standards consist of tools, policies, security concepts, security assurances, guidelines, risk management approaches, best practices, safeguards, and technologies. But they have, to one degree or another, a significant drawback – the complexity of transforming the results of information security assessment according to these standards into security guarantees with any wide international recognition. In the context of globalization, this significantly degrades the cybersecurity quality.*

*The main hypothesis of research is that the cybersecurity quality can be improved by converging towards a common methodology that is based on agreed international standards and international best practice for certification. The question of the key role of cybersecurity for operational technologies, which become the basis for Economy 4.0 and are now considered as a new frontier of cybersecurity, is considered. The need to create a system and schemes for certification of OT cybersecurity based on international and European certification principles is shown. A hierarchical model of cybersecurity certification system assessment standards and a hierarchical model of agreements on mutual recognition of cybersecurity certificates have been developed, which will allow a systematic approach to the creation of a system and schemes for OT cybersecurity certification. This provides an opportunity for developers of systems and certification schemes to form OT cybersecurity certification systems based on the principles of wide cross-border recognition of OT cybersecurity certificates.*

**Keywords:** *cybersecurity system, conformity assessment system, hierarchical model, cybersecurity certification scheme.*

Received date: 09.10.2020

Accepted date: 26.11.2020

Published date: 26.02.2021

© The Author(s) 2021

This is an open access article under the CC BY license

(<http://creativecommons.org/licenses/by/4.0>)

## 1. Introduction

Network and information systems with related services play a central role in society. It is important for economic and social activities, in particular for the functioning of the internal market, that they are reliable and safe. The scale, frequency and impact of information security incidents are growing and pose a significant threat to the smooth operation of network and information systems. Such cases affect the conduct of economic activities, cause significant financial losses, undermine user confidence and cause great harm to the economy [1].

One of the directions in ensuring the cybersecurity of the modern digital economy should be, along with the cybersecurity of IT technologies, the cybersecurity of operations technologies (OT technologies) systems, such as critical infrastructure and intelligent systems, as well as processes that ensure the functioning these systems. Among OT technologies, cybersecurity of industrial automation and control systems (IACS) occupies a special place, which is an important part of most critical infrastructures and critical services.

The process of transformation of society towards Industry 4.0 will lead to an even greater dependence on such systems. Experience has already shown that their cyber infiltration can be used to create a huge impact on critical infrastructure and further impact on the economy and people's lives. In practice, cyberattacks on critical infrastructures are actually cyberattacks on their IACS.

Therefore, it is extremely important to take all possible measures to improve the IACS cybersecurity level. To build an IACS cybersecurity, it is necessary to provision and assemble properly the IACS cybersecurity components, be it hardware or software.

At this stage, it is important to focus on the certification/conformity assessment of the individual IACS components to ensure that the cybersecurity requirements of each of these components are met as building blocks of the entire IACS. And by approaching component-based certification/conformity assessment, it is possible to define different security and assurance requirements for different elements of the overall IACS, depending on the system design, intended use and operating environment, and the

defined security system. In the EU, the Cybersecurity Component Certification Thematic Group, IACS TG, has been operating since 2014, which focuses on the cybersecurity certification of industrial automation components and control systems. The IACS TG has already developed for the EU common features (Framework) for the cybersecurity certification of IACS components, which will comply with EU cybersecurity legislation [2, 3]. The certification approach is an instance of the risk-based safety assessment methodology presented by ETSI based on ISO 31000 and the ISO 29119 software testing standard, reviewed in [4]. A study on the EU Cybersecurity Directive, the need to develop cybersecurity certification schemes, and the obligations of Member States with respect to their respective national strategies and cooperation in these matters at the EU level are presented in [5]. Certification systems and schemes can generally operate at the international, regional, national, subnational or sectoral level [6]. These circumstances will require developers of OT cybersecurity certification systems and schemes to apply a certain methodological framework. This is most problematic in the case of international recognition of cybersecurity certificates obtained from national level certification bodies. At the national level, each country has its own unique conditions for this. However, national OT cybersecurity certification schemes must ensure international recognition of their results.

In the future, the material will be presented on the example of Ukraine, without limiting the possibility of its use for any other country.

Therefore, it is relevant to create methodological support for the development of national systems and schemes for OT cybersecurity certification with cross-border recognition of certification results.

Thus, *the object of research* is the system and schemes of conformity assessment (certification) of OT cybersecurity, as a set of rules and procedures describing the objects of certification, determine the specified requirements and provide a methodology for certification. *The aim of research* is to develop models of assessment standards for the cybersecurity certification system and agreements on mutual recognition of cybersecurity certificates, which will allow a systematic approach to the creation of procedures for assessing the compliance of OT cybersecurity with cross-border recognition of certificates.

## 2. Methods of research

The main hypothesis of research is the assumption that the effectiveness of cybersecurity governance can be achieved through convergence towards a common methodology that is based on agreed international standards and international best practice for certification. At the same time, it is assumed that such an approach will require certain improvement in the legal and regulatory framework for cybersecurity in Ukraine.

Research is based on methods:

- dialectical – in identifying and researching the relationships between participants in the certification processes for OT cybersecurity, determining factors and conditions at the national level that will affect their international recognition;
- empirical – when collecting information in the pro-

cess of analyzing international standards that can be used for certification of OT cybersecurity, the state of the national accreditation body of Ukraine and international systems for ensuring mutual recognition of certification results;

- system-analytical – for the formation of an organizational and technical mechanism for certification of OT cybersecurity, the development of models of assessment standards for OT cybersecurity certification and agreements on the mutual recognition of certification results;

- generalizing and comparative – to assess the current mechanisms of international accreditation systems for certification bodies and to study the possibilities of applying international experience for certification of OT cybersecurity for the national cybersecurity system of Ukraine.

## 3. Research results and discussion

To date, the issue of cybersecurity in Ukraine is regulated by a number of regulatory legal acts [7, 8]. Among them, the most relevant are:

1. Decree of the President of Ukraine dated March 15, 2016 No. 96/2016 on the implementation of the «Cybersecurity Strategy of Ukraine».

2. Law of Ukraine «On the basic principles of ensuring the cybersecurity of Ukraine» dated October 5, 2017.

These documents note that the development of a safe cyberspace should primarily consist in the harmonization of regulatory documents, in the protection of information, information system and cybersecurity in accordance with international standards and EU and NATO standards.

In the work, first of all, international standards that can be used for OT cybersecurity certification are analyzed and defined.

Among others, the requirements for components, products and equipment used as elements of an OT system can be based on the international IEC and ISO standards that relate to IACS standards, such as:

1. IEC 62443-1-1 ed. 2: Terminology, concepts and models.
2. IEC 62443-2-1 ed. 2: Drawing up a program to ensure the security of the control system and industrial automation.
3. IEC 62443-2-3: Patch management in the IACS environment.
4. IEC 62443-2-4: Security program requirements for IACS service providers.
5. IEC 62443-2-2: IACS protection levels.
6. IEC 62443-3-2: Assessment of security risks and system design.
7. IEC 62443-3-1: Industrial cybersecurity program.
8. IEC 62443-4-1: Requirements for life cycle safety in product development.
9. IEC 62443-3-3-3: Requirements for system security and security level.
10. IEC 62443-4-2: Requirements for technical safety of IACS components.

Requirements for personal competence in the field of cybersecurity can be based on existing international ISO and IEC standards in this area, such as

ISO/IEC 27021: 2017 Information technology – Methods and means of ensuring security – requirements for the competence of information security management systems (ISMS) specialists.

The requirements for OT processes can be based on the relevant international standards IEC and ISO:

1. IEC 62443-4-1: Life cycle safety requirements for product development.
2. IEC 62443-2-1: IACS security programming.
3. IEC 62443-2-2: IACS protection levels.
4. IEC 62443-2-4: Security program requirements for IACS service providers.
5. IEC 62443-3-2: Assessment of security risks and system design.

Let's note that some of these standards are still under development.

At the same time, the presence of a large number of cybersecurity standards does not provide national regulators with answers to the questions of the choice and procedure for their application in the systematized legal and regulatory framework for IT cybersecurity. The situation is further complicated by the national status of these standards, guarantees of their correct implementation at all stages of the OT life cycle, risks and trust in OT, and the like.

The article investigates the methodology of a systematic approach to the cybersecurity of labor protection within the framework of the general system of technical regulation. It differs from other cybersecurity methodologies in that, in addition to purely technical cybersecurity issues, it involves an analysis of cybersecurity compliance assessment (certification) needs. The need for certification of cybersecurity, in turn, will require taking into account the state of development of the national system of technical regulation or formulate tasks to improve the national system of technical regulation, taking into account the needs for cybersecurity. This convergence towards a common methodology, which is based on agreed international standards and international best practice in conformity assessment, has several advantages. In particular, where third party conformity assessment is used to demonstrate the conformity of components and technologies, competencies and qualifications of individuals, this facilitates the recognition of this conformity in international trade and the movement of qualified personnel. It is also a universal methodology applicable to many different technical systems in different sectors of the economy that need to be adjusted. It is especially important to apply this methodology by national regulators responsible for cybersecurity issues [8].

The article highlights the key elements of government regulatory processes that can be used by authorities and policymakers, especially in sectors where cybersecurity regulations do not currently exist. The developed hierarchical models of assessment standards and international agreements in the field of technical regulation can become the basis for the development of national systems and schemes for certification of cybersecurity. They can also become the basis for normative documents on cybersecurity, meaning, first of all, ensuring cross-border recognition of the results of assessing the cybersecurity compliance of OT technologies.

### **3.1. OT cybersecurity conformity assessment (certification)**

Conformity assessment (certification) is a demonstration that specified requirements are met (conformity assessment includes activities such as testing, inspection, validation, verification, certification and accreditation). Specified requirement – a need or expectation that is specified (the specified requirements can be stated in regulatory documents such as regulations, standards and technical specifications. The specified requirements can be detailed and general) [6].

### **3.2. Accreditation of conformity assessment bodies**

As stated above, the convergence towards a common OT cybersecurity certification methodology is based on agreed international standards and international best practice in conformity assessment, which allows for the widespread use of mechanisms for the mutual recognition of certificates of conformity. The best international practice of conformity assessment is primarily based on the international system of accreditation of conformity assessment bodies, it is desirable to apply it to the OT cybersecurity.

Accreditation is the process by which an authoritative body gives formal recognition of the competence of an organization or individual to perform specific tasks [9]. Within the framework of technical regulation, the accreditation body evaluates the competence of certification bodies for products, services and processes, management systems, inspection and personnel, testing and calibration laboratories. Official recognition, called «accreditation», proves to clients and users of services the competence of these organizations. Accreditation is often mandated by government accreditation, which can provide recognition for its accreditation services through the International Accreditation Forum (IAF) and the International Laboratory Accreditation Committee (ILAC).

IAF and ILAC are global conformity assessment organizations of accreditation bodies and other bodies interested in conformity assessment in the field of management systems, products, services, personnel, testing laboratories and the like. Their main function is to develop uniform worldwide conformity assessment programs [10, 11].

IAF and ILAC shall promote and govern the recognition of Bilateral or Multilateral Agreements or Arrangements (MRAs/MLA) whereby the parties to them agree to mutually recognize the results of testing, inspection, certification or accreditation. MRAs/MLAs are today an important step towards optimizing or reducing the number of certifications for products, services, systems, processes and materials, especially in international activities.

It should also be noted that the IAF/ILAC global system operates through regional accreditation organizations. Their geographical location is shown in Fig. 1.

For Ukraine, the regional accreditation organization is the European Organization for Accreditation (EA). It is EA in the IAF/ILAC system that is the primary barrier that must be overcome in order to sign MRA/MLA agreements with the aim of cross-border recognition of cybersecurity certificates.

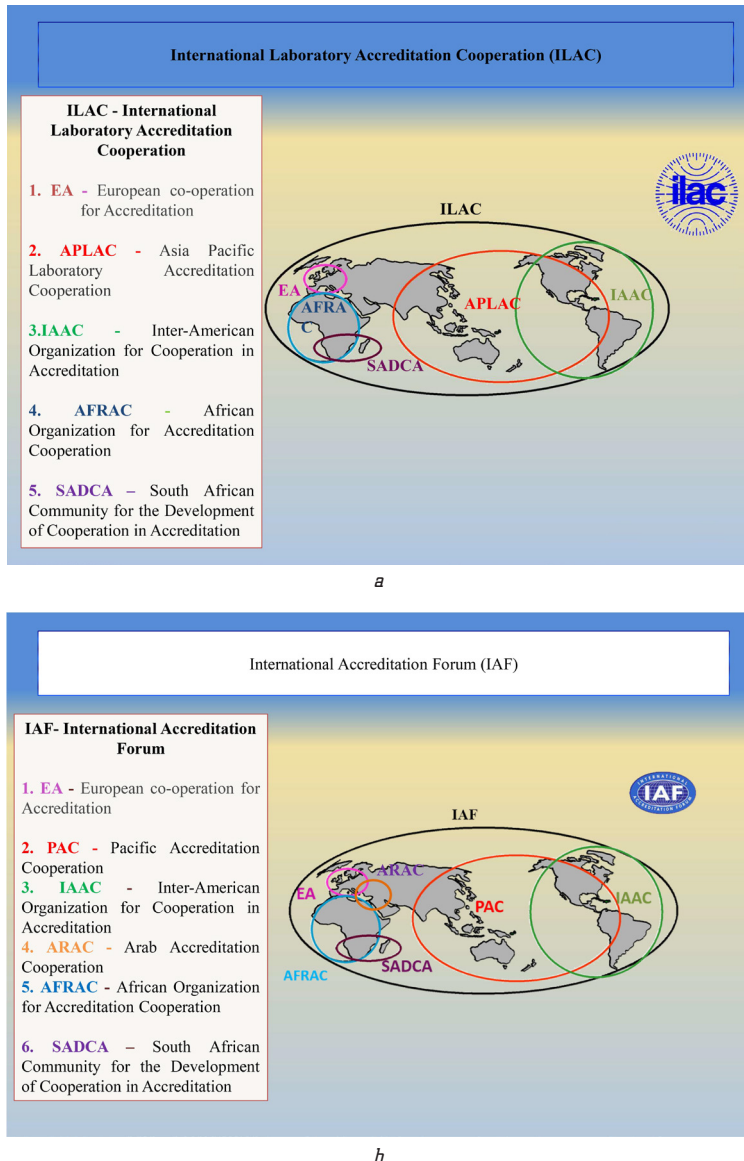


Fig. 1. International organizations: a – ILAC; b – IAF

### 3.3. Cybersecurity certification system for OT technologies for Ukraine

OT cybersecurity certification in the national cybersecurity system of Ukraine primarily requires the creation of an ICT cybersecurity conformity assessment system (hereinafter – the Certification System).

Conformity assessment system is a set of rules and procedures for the management of similar or related conformity assessment schemes. The conformity assessment system can operate at the international, regional, national, subnational or sectoral level. The assessment (confirmation) of compliance with the established requirements by an impartial third party is called certification [6]. In what follows, instead of the generalized concept of «conformity assessment» let's use the term «certification». The content of the certification system is the organization and management of related certification schemes, the general assessment methods that underlie certification [6].

Related schemes for assessing compliance with cybersecurity certification (hereinafter – the Certification Scheme) can be various applications of conformity assessment pro-

cedures, depending on the relationship to certain OT technologies (for example, IACS, IoT, cloud services, etc.). A certification scheme should use specific rules, procedures and management that may be specific to that scheme or which may be defined in a product certification system applied to a number of schemes. The certification system should be created taking into account all important factors and conditions. As for certification of OT cybersecurity for Ukraine, among them it is necessary to highlight three system-forming factors:

1. The need to comply with the requirements of the Ukraine-EU Agreement and Article 56 of this Agreement.

2. Signed agreements on recognition in the field of accreditation of certification bodies.

3. The presence in the EU of Regulation 2019/881 on certification of cybersecurity, the basic principles of which will eventually have to be implemented in the national cybersecurity system of Ukraine.

Taking into account heterogeneous essential and rapid factors for creating a certification system for OT cybersecurity is possible by introducing unified models based on global mechanisms for eliminating technical barriers to trade and the current state of the technical regulation system of Ukraine:

- hierarchical model of assessment standards of the Cybersecurity Certification System;
- hierarchical model of agreements on mutual recognition of cybersecurity certificates.

The general hierarchical model of assessment standards of the Cybersecurity Certification System (hereinafter – the Model of Standards) is shown in Fig. 2. The model allows to streamline the definition and application of standards or other regulations, standards and schemes with possible combinations for the development of certification schemes.

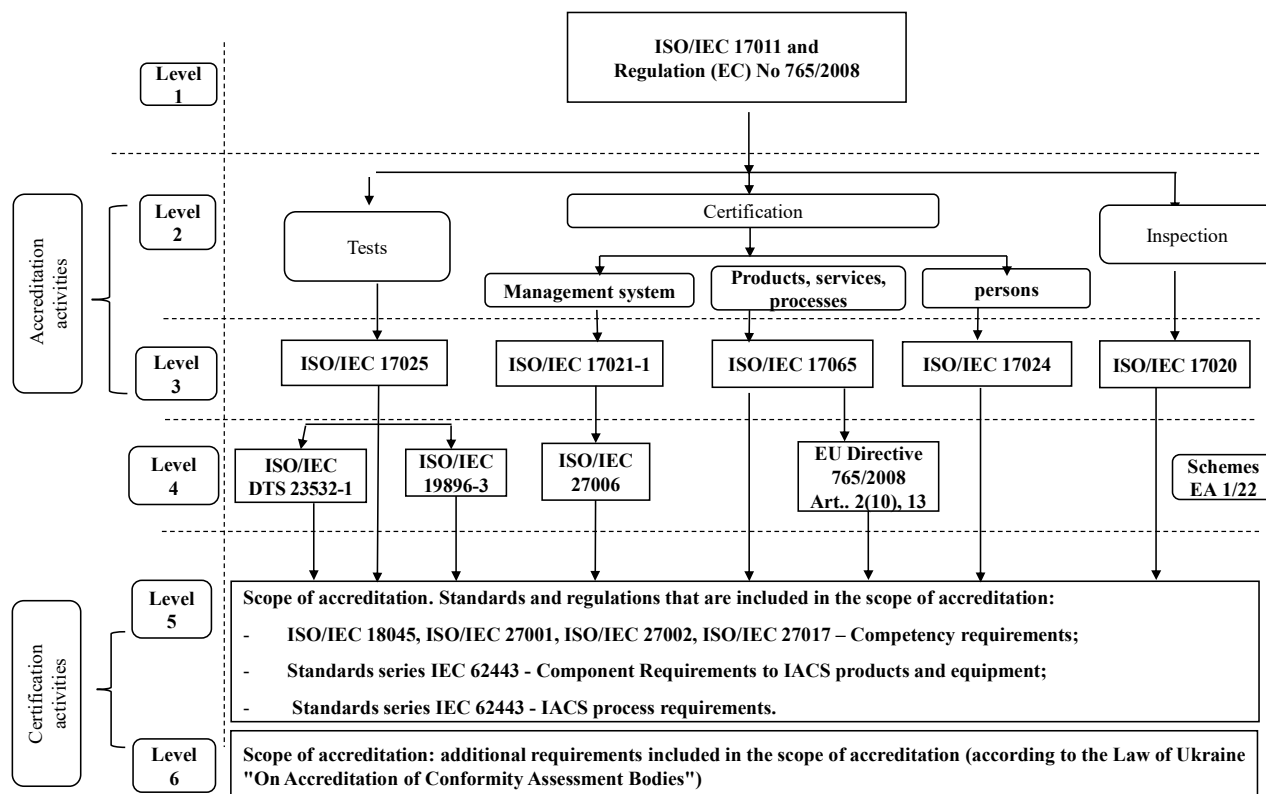
The model consists of 6 levels, the systematic distribution of assessment standards for which creates flexibility for developers of cybersecurity certification schemes.

Level 1 – requirements for accreditation bodies, accreditation bodies involved in cybersecurity certification. Defined in ISO/IEC 17011, Regulation (EC) 765/2008 and, if necessary, additional requirements defined in binding EA documents and in IAF and/or ILAC documents (approved by EA as mandatory for EU) [10, 11].

Level 2 – conformity assessment activities of CABs (conformity assessment bodies), which accreditation bodies grant accreditation in accordance with the standards included up to level 3 (hereinafter – conformity assessment activities). This is usually defined in the certification scheme. For certification of OT cybersecurity, depending on the certification scheme, the following may be involved:

- certification bodies for products, services and processes;
- certification bodies for management systems;
- personnel certification bodies;
- testing laboratories;
- inspection bodies.





**Fig. 2.** Hierarchical model of assessment standards of the cybersecurity certification system of operational technologies

Level 3 – harmonized standards (or other normative documents) containing general requirements for CABs performing cybersecurity compliance assessment activities included up to level 2 (hereinafter conformity assessment standards). These are the following assessment standards: ISO/IEC 17025; ISO/IEC 17020; ISO/IEC 17065; ISO/IEC 17021-1; ISO/IEC 17024.

Level 4 – documents containing additional criteria to the level 3 standards. Level 4 only applies where documents exist to complement the Level 3 standards (meaning that Level 5 is often directly related to the Level 3 standard).

Such documents for the EU: industry standards or other regulatory documents (hereinafter industry standards); sectoral schemes as specified in Regulation (EC) 765/2008 Articles 2 (10) and 13; Conformity assessment schemes according to EA-1/22 (hereinafter schemes).

Thus, the industry standard that will no doubt be in the system is ISO/IEC 27006:2015. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.

It is also highly probable that additional criteria of EU Regulation 2019/881 are included in the Cybersecurity Certification System.

Level 5 – scope of accreditation of the certification body: standards or other normative documents used by the accredited CAB of conformity to a specific accredited scope of conformity assessment. The framework is based on the standards discussed in clause F. May include, for example, specific test methods and specific management system requirements (e. g.: ISO/IEC 27001), ISO/IEC 27021:2017 – Competence requirements for information security management systems (ISMS) professionals.

Level 6 – scope of accreditation of the certification body: additional requirements for the scope of accreditation that may be established in the state. Defined in the Law of Ukraine «On Accreditation of Conformity Assessment Bodies», Article 1 [12].

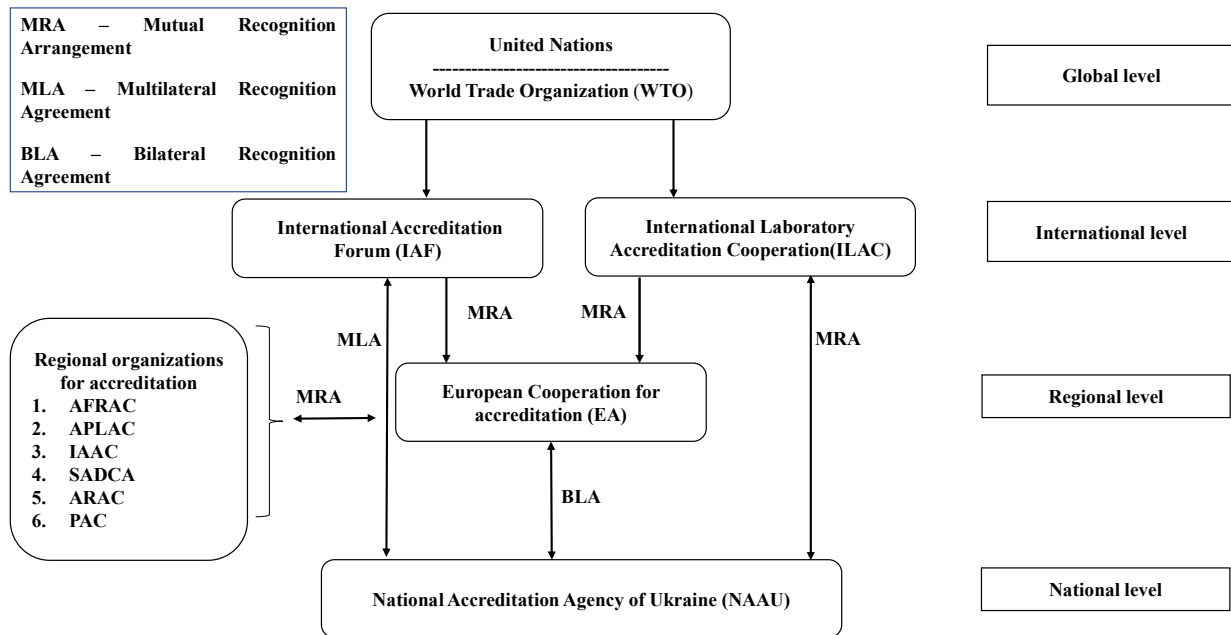
The proposed 6-level Hierarchical Model for OT Cybersecurity Certification System Assessment Standards is a toolkit that provides the ability to create flexible cybersecurity certification schemes with ensuring cross-border recognition of cybersecurity conformity assessment results (testing and certification).

The hierarchical model of agreements on mutual recognition of cybersecurity certificates should reflect the level and corresponding scope (scope) of recognition of the results of activities by international accreditation organizations for the national accreditation body. The achievability of levels (in fact) and the scope for the national accreditation body determines the scope of recognition of the results of cybersecurity certification, forming mechanisms for the mutual recognition of certificates for the cybersecurity certification system.

Fig. 3 shows a developed four-level hierarchical model of agreements on mutual recognition of cybersecurity certificates (MRA for IAF and ILAC), where the National Accreditation Body of Ukraine – National Accreditation Agency of Ukraine (hereinafter – NAAU) is represented at the national level.

The model contains national, regional, international and global levels, represented by the respective accreditation organizations and types of recognition agreements.

To operate the model in the development of the OT certification system, the necessary application is the Agreements themselves and the areas of recognition of accreditation activities defined in them.



**Fig. 3.** Hierarchical model of agreements on mutual recognition of certificates of cybersecurity of operational technologies

The model has a methodological significance and allows, when developing a system and schemes for cybersecurity certification, to be determined with the content of the corresponding sections on assessment standards, levels of guarantees for cybersecurity certificates, CAB accreditation, mutual recognition of certificates, etc. [13].

To create an effective system for assessing the cybersecurity of ICT in Ukraine, it is advisable to analyze the agreements in force for the NAAU in the EA and IAF/ILAC systems. It should be noted that such an analysis can give the following scenarios for creating an OT cybersecurity certification system in the National Cybersecurity System of Ukraine:

- the existence of agreements is sufficient to create a system and certification schemes in accordance with


international and EU and NATO standards;

- the existence of agreements is insufficient and requires additional efforts on the part of Ukraine and the NAAU in the direction of expanding the scope of recognition in the EA and IAF/ILAC system;
- the existence of agreements is insufficient and requires the creation of a system at the national or sectoral level without the intention of cross-border recognition of certification results, but in accordance with international and EU and NATO standards.

The agreements that define the status of the National Body of Ukraine for CAB accreditation for cross-border recognition of activities are shown in Fig. 4. It also contains excerpts from the IAF and ILAC websites indicating the areas of accreditation covered by the respective agreements.

<https://ilac.org/signatory-detail/?id=124>


**ILAC MRA SIGNATORY CONTACT DETAILS**



**Name** National Accreditation Agency of Ukraine  
**Acronym** NAAU  
**Membership Category** Full Member (ILAC MRA signatory)  
**Economy** UKRAINE  
**ILAC MRA Scope:** Calibration: ISO/IEC 17025 24 Sep 2014  
 Testing: ISO/IEC 17025 24 Sep 2014  
 Inspection: ISO/IEC 17020 11 Dec 2014  
**Contact Name** Dr Viktor Gorytsky  
**Phone** +38 044 369 3469  
**Email** [office@naau.org.ua](mailto:office@naau.org.ua)  
**Website** <http://www.naau.org.ua>

**IAF MEMBERS & SIGNATORIES**  
 Accreditation Body Member

**Economy:** Ukraine  
**Body:** **National Accreditation Agency of Ukraine (NAAU)**  
**Contact:** Dr. Viktor Gorytsky  
 Chairman



National Accreditation Agency of Ukraine  
 18/7 Generala Almazova Street  
 01133 Kyiv  
 Ukraine  
 Telephone: +380 (44) 369 34 70  
 Facsimile: +380 (44) 369 34 70  
 Email: [office@naau.org.ua](mailto:office@naau.org.ua)  
 Website: <http://naau.org.ua>  
 Code of Conduct Adopted: 16 June 2017

**IAF MLA**  
 Main scopes  
 Management system certification - ISO/IEC 17021-1  
 Product certification - ISO/IEC 17065 - 06 Aug 2017  
 Certifications of persons - ISO/IEC 17024 - 06 Aug 2017  
 Sub scopes  
 Level 4  
 MS: ISO/IEC TS 17021-3 - 06 Aug 2017  
 MS: ISO/IEC TS 17021-2 - 06 Aug 2017  
 MS: ISO/TS 22003 - 05 Apr 2018  
 MS: ISO/IEC 27006 - 05 Apr 2018  
 MS: ISO 50003 - 05 Apr 2018  
 Level 5  
 MS: ISO 9001 - 06 Aug 2017  
 MS: ISO 14001 - 06 Aug 2017  
 MS: ISO 22000 - 05 Apr 2018  
 MS: ISO/IEC 27001 - 05 Apr 2018  
 MS: ISO 50001 - 05 Apr 2018  
 MS: ISO 13485 - 05 Apr 2018

**Fig. 4.** Agreements and areas of recognition: *a* – MRA ILAC; *b* – MLA IAF

Analysis of the current status of the NAAU agreements and the areas of accreditation in which these Agreements operate makes it possible to identify possible assessment standards and other standards to fill the hierarchical model of standards and form a system of OT cybersecurity certification.

#### 4. Conclusions

In the course of the study, based on the standards and systems that are used for certification of products in the ILAC/IAF system, a Hierarchical Model of Assessment Standards of the OT Cybersecurity Certification System and a Hierarchical Model of Agreements in the International ILAC/IAF/EA System on the mutual recognition of cybersecurity certificates have been developed.

The research results will be useful to developers and owners of OT cybersecurity certification systems and schemes as elements of a common methodology that is based on agreed international standards and international best practice in conformity assessment in the ILAC/IAF system.

Also, the research results will be of interest to national regulatory authorities in the areas of cybersecurity and technical regulation to determine national needs for assessment standards, certification schemes, the scope of international recognition of the national accreditation body.

#### References

1. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6.07.2016 concerning measures for a high common level of security of network and information systems across the Union* (2016). Available at: <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>
2. *The IACS Cybersecurity Certification Framework (ICCF)* (2018). Available at: <https://erncip-project.jrc.ec.europa.eu/documents/iacs-cybersecurity-certification-framework-iccf>
3. *Regulation (EU) 2019/881 of the European Parliament and*

*of the Council of 17.04.2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)* (2019). Available at: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

4. Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces*, 62, 64–83. doi: <http://doi.org/10.1016/j.csi.2018.08.003>
5. Markopoulou, D., Papakonstantinou, V., de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, 35 (6), 105336. doi: <http://doi.org/10.1016/j.clsr.2019.06.007>
6. *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy* (2017). Zakon Ukrainy No. 2163-VIII. 05.10.2017. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
7. *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiu kiberbezpeky Ukrainy»* (2016). Ukaz Prezidenta Ukrainy; Stratehiia No. 96/2016. 15.03.2016. Available at: <https://www.president.gov.ua/documents/2422016-20141>
8. *ISO/IEC 17000:2020 Conformity assessment – Vocabulary and general principles* (2020). Committee on conformity assessment, 23. Available at: <https://www.iso.org/standard/73029.html>
9. *Pro tekhnichni rehlementy ta otsinku vidpovidnosti* (2015). Zakon Ukrainy No. 124-VIII. 15.01.2015. Available at: <https://zakon.rada.gov.ua/laws/show/3164-15#Text>
10. *International Accreditation Forum*. Available at: <https://www.iaf.nu/>
11. *International Laboratory Accreditation Cooperation*. Available at: <https://ilac.org/>
12. *Pro akredytatsiiu orhaniv z otsinky vidpovidnosti* (2001). Zakon Ukrainy No. 2407-III. 17.05.2001. Available at: <https://zakon.rada.gov.ua/laws/show/2407-14#Text>
13. *ISO/IEC 17067:2013 Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes* (2013). Committee on conformity assessment, 13. Available at: <https://www.iso.org/standard/55087.html>

**Olena Tsvilii**, Senior Lecturer, Department of Telecommunications, O. S. Popov Odesa National Academy of Telecommunications, Odessa, Ukraine, e-mail: [o.tsvilii@ukr.net](mailto:o.tsvilii@ukr.net), ORCID: <http://orcid.org/0000-0002-4414-9881>